ICS 43.430
CCS T 35

中华人民共和国国家标准

GB/T 34590.3—XXXX
代替 GB/T 34590.3-2017

道路车辆 功能安全
第3部分：概念阶段

Road vehicles—Functional safety—Part 3:Concept phase

(ISO 26262-3:2018，MOD)

（征求意见稿）

（本草案完成时间：2021年4月1日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

GB/T 34590-XXXX《道路车辆 功能安全》分为以下部分：

——第 1 部分：术语；

——第 2 部分：功能安全管理；

——第 3 部分：概念阶段；

——第 4 部分：产品开发：系统层面；

——第 5 部分：产品开发：硬件层面；

——第 6 部分：产品开发：软件层面；

——第 7 部分：生产、运行、服务和报废；

——第 8 部分：支持过程；

——第 9 部分：以汽车安全完整性等级为导向和以安全为导向的分析；

——第 10 部分：指南；

——第 11 部分：半导体应用指南；

——第 12 部分：摩托车的适用性。

本文件为GB/T 34590-XXXX的第3部分。

本文件代替GB/T 34590.3-2017《道路车辆 功能安全 第3部分：概念阶段》,与GB/T 34590.3-2017相比，除结构调整和编辑性改动外，主要技术变化如下：

——修改了标准适用范围，由“量产乘用车”扩大到“除轻便摩托车外的量产道路车辆”；

——新增了对商用车辆的相关要求和示例、对摩托车的适应性要求等；

——修改了相关项定义的目的（见 5.1）；

——修改了应给出相关项要求的内容（见 5.4.1）；

——修改了定义相关项的边界、接口以及其他相关项及要素交互关系的假设时应考虑的内容（见 5.4.2）；

——删除了安全生命周期启动的内容（见 2017 版的第 6 章）；

——修改了危害分析和风险评估的支持信息的要求（见 6.3.2，2017 版,7.3.2）；

——修改了描述危害事件发生的运行场景的要求（见 6.4.2.1，2017 版的 7.4.2.1）；

——修改了危害识别时确定危害的要求（见 6.4.2.2，2017 版的 7.4.2.2.1）；

——修改了处理超出 GB/T 34590 范围的危害的要求（见 6.4.2.4，2017 版的 7.4.2.2.5）；

——增加了严重度分级应考虑因素的要求（见 6.4.3.3）；

——修改了仅限于物体损伤并不涉及人员伤害的危害的严重度等级分析要求（见 6.4.3.4，2017 版的 7.4.3.3）；

——修改了预估危害事件可控性的要求（见 6.4.3.8，2017 版的 7.4.3.7）；

——修改了不影响车辆安全运行的危害的可可用性评估要求（见 6.4.3.9，2017 版的 7.4.3.8）；

——修改了 QM 等级的要求（见 6.4.3.10、6.4.3.11、表 4，2017 版的 7.4.4.1、表 4）；

——修改了确定安全目标的要求（见 6.4.4.1，2017 版的 7.4.4.3）；

——增加了危害识别和风险评估过程中应识别使用到的或从中得出的假设的要求（见 6.4.4.4）；

——增加了 T&B 车辆危害分析和风险评估的差异管理要求（见 6.4.5）；

——修改了对危害分析和风险评估进行验证的要求（见 6.4.6.1，2017 版的 7.4.5）；
——修改了危害分析和风险评估的工作成果（见 6.5，2017 版的 7.5）；
——修改了功能安全概念的目的（见 7.1，2017 版的 8.1）；
——修改了功能安全概念的总则要求（见 7.2，2017 版的 8.2）；
——修改了功能安全概念的支持信息（见 7.3.2，2017 版的 8.3.2）；
——修改了功能安全要求的导出的内容（见 7.4.2.1，2017 版的 8.4.2.1）；
——修改了功能安全要求应定义的策略的要求（见 7.4.2.3，2017 版的 8.4.2.5）；
——增加了定义功能安全要求时应考虑的内容（见 7.4.2.4）；
——修改了对驾驶员或其他人员的必要行动进行假设的要求（见 7.4.2.7，2017 版的 8.4.2.6）；
——修改了功能安全要求分配的要求（见 7.4.2.8，2017 版的 8.4.3.1）；
——修改了功能安全概念依赖于外部措施时的要求（见 7.4.2.10，2017 版的 8.4.3.3）；
——修改了安全确认准则的要求（见 7.4.3，2017 版的 8.4.4）；
——将附录 A 的内容进行了适应性修改（见附录 A）；
——修改了危害分析和风险评估总则的要求（见附录 B.1）；
——修改了严重度等级示例的内容（见表 B.1）；
——修改了暴露概率示例与解释的内容（见附录 B.3）；
——修改了基于运行场景持续时间以及运行场景频率的暴露概率等级示例的内容（见表 B.2、表 B.3），增加了 T&B 车辆基于运行场景持续时间以及运行场景频率的暴露概率等级示例的内容（见表 B.4、表 B.5）；
——修改了驾驶员或者潜在涉险人员可能控制的危害事件示例的内容（见表 B.6，2017 版的表 B.4）。

本文件使用重新起草法修改采用了ISO 26262-3:2018《道路车辆 功能安全 第3部分:概念阶段》。

本文件与ISO 26262-3：2018的技术性差异及其原因如下：

——关于规范性引用文件，本文件做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第 2 章“规范性引用文件”中，具体调整如下：

- 用修改采用国际标准的GB/T 34590.1-XXXX代替ISO 26262-1：2018；
- 用修改采用国际标准的GB/T 34590.2-XXXX代替ISO 26262-2：2018；
- 用修改采用国际标准的GB/T 34590.4-XXXX代替ISO 26262-4：2018；
- 用修改采用国际标准的GB/T 34590.8-XXXX代替ISO 26262-8：2018；
- 用修改采用国际标准的GB/T 34590.9-XXXX代替ISO 26262-9：2018。

——附录 B 表 B.2，在 E4 等级下新增“城市道路”道路类型示例，以适应我国的道路场景；
——6.1 列项 b）中，增加定义接受准则的要求。
——修改了 7.1 的列项 e）中关于接受准则的要求。
——增加了 7.4.4.1 的列项 b）中对于满足接受准则的要求。

本文件做了下列编辑性修改：

——将国际标准中的“本国际标准”改为“本文件”；
——删除国际标准的前言；
——修改国际标准的引言及其表述。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会（SAC/TC114）归口。

本文件起草单位：

本文件主要起草人：

本文件所代替文件的历次版本发布情况为：

——GB/T 34590.3,2017 年首次发布。

引　言

ISO 26262是以IEC 61508为基础，为满足道路车辆上电气/电子系统的特定需求而编写。

GB/T 34590修改采用ISO 26262，适用于道路车辆上由电子、电气和软件组件组成的安全相关系统在安全生命周期内的所有活动。

安全是道路车辆开发的关键问题之一。汽车功能的开发和集成强化了对功能安全的需求，以及对提供证据证明满足功能安全目标的需求。

随着技术日益复杂、软件和机电一体化应用不断增加，来自系统性失效和随机硬件失效的风险逐渐增加，这些都在功能安全的考虑范畴之内。GB/T 34590通过提供适当的要求和流程来降低风险。

为了实现功能安全，GB/T 34590-XXXX（所有部分）：

a) 提供了一个汽车安全生命周期（开发、生产、运行、服务、报废）的参考，并支持在这些生命周期阶段内对执行的活动进行剪裁；

b) 提供了一种汽车特定的基于风险的分析方法，以确定汽车安全完整性等级（ASIL）；

c) 使用 ASIL 等级来定义 GB/T 34590 中适用的要求，以避免不合理的残余风险；

d) 提出了对于功能安全管理、设计、实现、验证、确认和认可措施的要求；及

e) 提出了客户与供应商之间关系的要求。

GB/T 34590针对的是电气/电子系统的功能安全,通过安全措施(包括安全机制)来实现。它也提供了一个框架，在该框架内可考虑基于其它技术（例如，机械、液压、气压）的安全相关系统。

功能安全的实现受开发过程（例如，包括需求规范、设计、实现、集成、验证、确认和配置）、生产过程、服务过程和管理过程的影响。

安全问题与常规的以功能为导向和以质量为导向的活动及工作成果相互关联。GB/T 34590涉及与安全相关的开发活动和工作成果。

图1为GB/T 34590的整体架构。GB/T 34590基于V模型为产品开发的不同阶段提供参考过程模型：

——阴影”V”表示 GB/T 34590.3-XXXX、GB/T 34590.4-XXXX、GB/T 34590.5-XXXX、GB/T 34590.6-XXXX、GB/T 34590.7-XXXX 之间的相互关系；

——对于摩托车：

- GB/T 34590.12-XXXX的第8章支持GB/T 34590.3-XXXX；
- GB/T 34590.12-XXXX的第9章和第10章支持GB/T 34590.4-XXXX。

——以“m-n”方式表示的具体章条中，“m”代表特定部分的编号，“n”代表该部分章的编号。

示例：“2-6”代表 GB/T 34590.2-XXXX 的第 6 章。

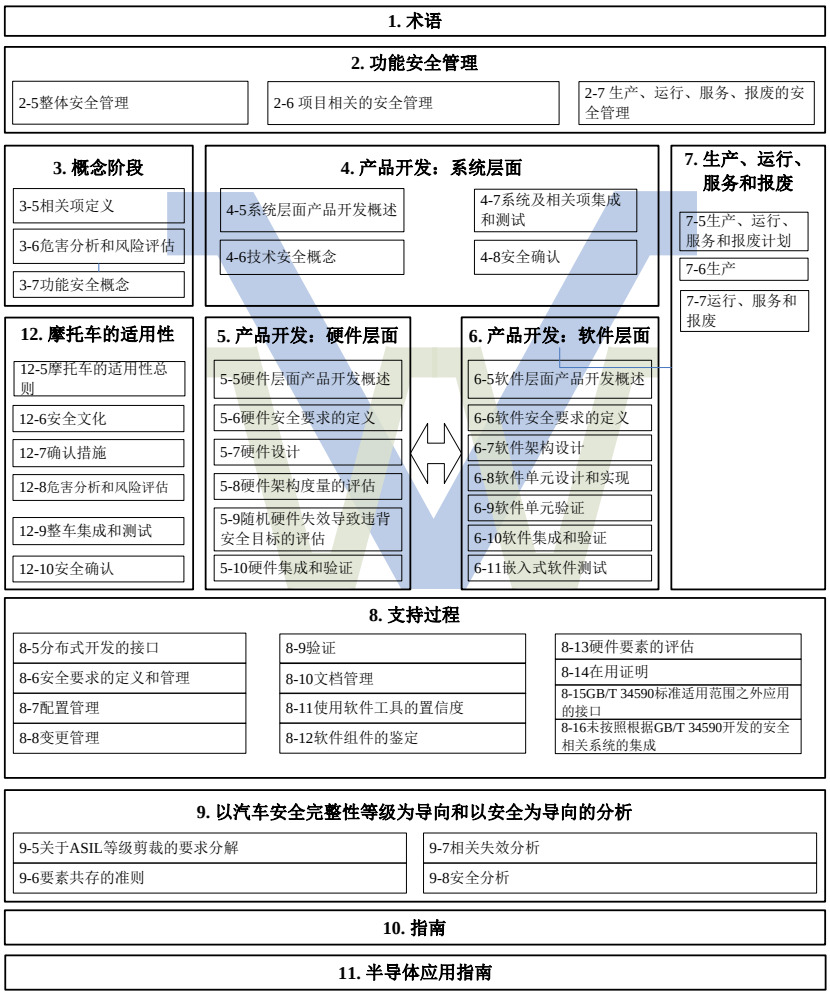


图1　GB/T 34590-XXXX 概览

道路车辆 功能安全
第3部分：概念阶段

1 范围

GB/T 34590的本文件规定了车辆在概念阶段的要求，包括：

——相关项定义；

——危害分析和风险评估；

——功能安全概念。

本文件适用于安装在除轻便摩托车外的量产道路车辆上的包含一个或多个电气/电子系统的与安全相关的系统。

本文件不适用于特殊用途车辆上特定的电气/电子系统，例如，为残疾驾驶者设计的车辆。

注：其他专用的安全标准可作为本文件的补充，反之亦然。

已经完成生产发布的系统及其组件或在本文件发布日期前正在开发的系统及其组件不适用于本文件。对于在本文件发布前完成生产发布的系统及其组件进行变更时，本文件基于这些变更对安全生命周期的活动进行裁剪。未按照本文件开发的系统与按照本文件开发的系统进行集成时，需要按照本文件进行安全生命周期的裁剪。

本文件针对由安全相关的电气/电子系统的功能异常表现而引起的可能的危害，包括这些系统相互作用而引起的可能的危害。本文件不针对与触电、火灾、烟雾、热、辐射、毒性、易燃性、反应性、腐蚀性、能量释放等相关的危害和类似的危害，除非危害是直接由安全相关的电气/电子系统的功能异常表现表现而引起的。

本文件提出了安全相关的电气/电子系统进行功能安全开发的框架，该框架旨在将功能安全活动整合到企业特定的开发框架中。本文件规定了为实现产品功能安全的技术开发要求，也规定了组织应具备相应功能安全能力的开发流程要求。

本文件不针对电气/电子系统的标称性能。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 34590.1-XXXX 道路车辆 功能安全 第1部分：术语(ISO 26262-1:2018,MOD)

GB/T 34590.2-XXXX 道路车辆 功能安全 第2部分：功能安全管理(ISO 26262-2:2018,MOD)

GB/T 34590.4-XXXX 道路车辆 功能安全 第4部分：产品开发：系统层面(ISO 26262-4:2018,MOD)

GB/T 34590.8-XXXX 道路车辆 功能安全 第8部分：支持过程(ISO 26262-8:2018,MOD)

GB/T 34590.9-XXXX 道路车辆 功能安全 第9部分：以汽车安全完整性等级为导向和以安全为导向的分析(ISO 26262-9:2018,MOD）

3 术语、定义和缩略语

GB/T 34590.1界定的术语、定义和缩略语适用于本文件。

4 要求

4.1 目的

本章规定了：

a) 如何符合 GB/T 34590-XXXX；

b) 如何解释 GB/T 34590-XXXX 中所使用的表格；及

c) 如何解释各章条基于不同的 ASIL 等级的适用性。

4.2 一般要求

如声明满足GB/T 34590-XXXX的要求时，应满足每一个要求，除非有下列情况之一：

a) 按照 GB/T 34590.2 的要求，安全活动的剪裁已经实施并表明这些要求不适用；或

b) 不满足要求的理由存在且是可接受的，并且按照 GB/T 34590.2 的要求对该理由进行了评估。

标有“注”或“示例”的信息仅用于辅助理解或阐明相关要求，不应作为要求本身且不具备完备性。

将安全活动的结果作为工作成果。应具备上一阶段工作成果作为“前提条件”的信息。如果章条的某些要求是依照ASIL定义的或可剪裁的，某些工作成果可不作为前提条件。

“支持信息”是可供参考的信息,但在某些情况下,GB/T 34590不要求其作为上一阶段的工作成果，并且可以是由不同于负责功能安全活动的人员或组织等外部资源提供的信息。

4.3 表的诠释

本文件中的表是规范性或资料性取决于上下文。在满足相关要求时，表中列出的不同方法有助于置信度水平。表中的每个方法是：

a) 一个连续的条目（在最左侧列以顺序号标明，如 1、2、3）；或

b) 一个选择的条目（在最左侧列以数字后加字母标明，如 2a、2b、2c）。

对于连续的条目，高度推荐和推荐的方法按照ASIL等级推荐予以使用。高度推荐或推荐的方法允许用未列入表中的其它方法替代,此种情况下，应给出满足相关要求的理由。如果可以给出不选择所有条目也能符合相应要求的理由，则不需要对缺省方法做进一步解释。

对于选择性的条目，应按照指定的ASIL等级对这些方法进行适当的组合，而与这些方法在表中是否列出无关。如果所列出的方法对于一个ASIL等级来说具有不同的推荐等级，宜采用具有较高推荐等级的方法。应给出选择组合方法或选择单一方法满足相应要求的理由。

注：在表中所列出方法的理由是充分的。但是，这并不意味着有倾向性或对未列到表中的方法表示反对。

对于每种方法，应用相关方法的推荐等级取决于ASIL等级，分类如下：

——“++”表示对于指定的 ASIL 等级，高度推荐该方法；

——“+”表示对于指定的 ASIL 等级，推荐该方法；

——“o”表示对于指定的 ASIL 等级，不推荐也不反对该方法。

4.4 基于 ASIL 等级的要求和建议

若无其它说明，对于ASIL A、 B、 C和D等级，应满足每一章条的要求或建议。这些要求和建议参照安全目标的ASIL等级。如果在项目开发的早期对ASIL等级完成了分解，按照GB/T 34590.9第5章的要求，应遵循分解后的ASIL等级。

如果GB/T 34590中ASIL等级在括号中给出，则对于该ASIL等级，相应的章条应被认为是推荐而非要求。这里的括号与ASIL等级分解无关。

4.5 摩托车的适用性

对于适用于GB/T 34590.12要求的摩托车的相关项或要素，GB/T 34590.12的要求替代本文件和GB/T 34590.2的相应要求。

4.6 卡车、客车、挂车和半挂车的适用性

对卡车、客车、挂车和半挂车的特殊规定以（T&B）来表示。

5 相关项定义

5.1 目的

本章的目的是：

a) 在整车层面对相关项进行定义和描述，包括功能，其与驾驶员、环境和其他相关项的依赖性和交互；及

b) 对充分理解相关项提供支持，以便执行后续阶段的活动。

5.2 总则

本章为建立相关项的定义列出了要求和建议，相关项的定义包括其功能、接口、环境条件、法规要求和危害。该定义为执行后续子阶段：“危害分析和风险评估”（本文件第6章）和“功能安全概念”（本文件第7章）的人员提供了关于相关项的充足信息。

注：表A.1提供了概念阶段的目的、前提条件和工作成果的概览。

5.3 本章的输入

5.3.1 前提条件

无。

5.3.2 支持信息

可考虑如下信息：

——任何与相关项有关的已有信息，例如产品理念、项目梗概、相关专利、预试验结果、来自前代相关项的文档、其他相关项的相关信息。

5.4 要求和建议

5.4.1 应给出相关项的要求，包括：

注1：在定义了安全目标和相应的ASIL等级后，这些要求可归类为是与安全相关的。

注2：如果当前没有功能性和非功能性的要求，可由本章的要求来促成该信息的生成。

a) 法规要求、国家标准和国际标准；

b) 整车层面的功能行为，包括运行模式或运行状态；

C) 所要求的质量、性能和功能的可用性（如果适用）；

d) 相关项的约束，例如：功能依赖性、与其他相关项的依赖性、运行环境；

e) 行为不足的潜在后果（如有），包括已知的失效模式和危害；及

注3：可包括已知的且包含类似相关项的安全相关事件。

f) 执行器的能力，或其假定的能力。

注4：在进行危害分析和风险评估的过程中，这些参数（例如：输出扭矩、所受的力、运行速度、亮度、音量）的值

或其估算值，对于确定影响的程度是必要的。在确定严重度等级和可控性等级时，需要将这些影响程度考虑在内。

5.4.2 定义相关项的边界、接口以及提出与其他相关项及要素交互关系的假设时，应考虑：

a) 相关项的要素；

注1：要素也可基于其他技术。

b) 相关项的行为对整车的影响的假设；

c) 其他相关项和要素要求本相关项提供的功能；

d) 本相关项要求其他相关项和要素提供的功能；

e) 功能在所涉及的系统和要素间的分配；及

f) 影响相关项功能的运行场景。

注2：随着整车功能复杂性的增加，相关项之间存在依赖性。一个相关项可以通过一组系统来实现，这些系统本身也实施了其他整车层面功能，即，这些系统也可以被视为不同相关项。

示例：自适应巡航控制和车道保持辅助的组合功能由一套制动系统、一套转向系统和一套驱动系统实现。在此示例中，制动系统实现了行车制动功能，其本身也可以视为一个相关项。

注3：如果开发范围是要素而不是相关项，请参阅GB/T 34590.2-XXXX，6.4.5.7。

5.5 工作成果

5.5.1 相关项定义，由 5.4 的要求得出。

6 危害分析和风险评估

6.1 目的

本章的目的是：

a) 识别并分类由相关项中的功能异常表现引起的危害事件;

b) 定义接受准则，包括危害行为的安全度量，以及由接受准则导出安全确认目标，用于评估残余风险;及

c) 制定防止危害事件发生或减轻危害程度的安全目标及其相应的 ASIL 等级，以避免不合理的风险。

6.2 总则

危害分析、风险评估和ASIL等级的确定用于确定相关项的安全目标。为此，根据相关项的潜在危害事件，对相关项进行评估。通过对危害事件进行系统性的评估确定安全目标及分配给他们的ASIL等级。ASIL等级的确定需要考虑严重度、暴露概率和可控性。严重度、暴露概率和可控性的确定基于相关项的功能行为，因而不一定需要知道相关项的设计细节。

6.3 本章的输入

6.3.1 前提条件

应具备以下信息：

——相关项定义，按照 5.5.1。

6.3.2 支持信息

可考虑如下信息：

——其他相关项的相关信息（来自外部）。

6.4 要求和建议

6.4.1 危害分析和风险评估的启动

6.4.1.1 应基于相关项定义进行危害分析和风险评估。

6.4.1.2 在危害分析和风险评估过程中，应对不含内部安全机制的相关项进行评估，即，在危害分析和风险评估过程中不应考虑将要实施或已经在先前相关项中实施的安全机制。

注1：在对相关项进行评估过程中，可用的且充分独立的外部措施是有益的。

示例：如果电子稳定性控制被证明是可用的，并且与被评估的相关项充分独立，那么其能够通过增加驾驶员的可控性来减轻底盘系统失效的影响。

注2：相关项中将要或已经实施的安全机制是功能安全概念的一部分。

6.4.2 场景分析和危害识别

6.4.2.1 应对相关项的功能异常表现导致一个危害事件发生时所处的运行工况及运行模式进行描述，包括正确的使用车辆和合理可预见的不正确使用车辆的情况。

注1：运行场景描述了假定相关项是以安全的方式运行的条件。

注2：由相关项非失效情况下的行为导致的危害，不属于本文件的范围。

6.4.2.2 应基于相关项可能的功能异常表现系统性地确定危害。

注1：FMEA方法和HAZOP适用于支持相关项层面的危害识别。这些可以通过头脑风暴、检查表、质量历史记录和现场研究来支持。

注2：通过建立外部措施以减轻货物运输过程带来的额外风险的责任不属于GB/T 34590的范围。因此，与货物运输相关的额外风险不属于危害分析和风险评估的部分。

6.4.2.3 应在整车层面定义由相关项的功能异常表现导致的危害。

注1：通常，每一个危害有多种与相关项的实现相关的潜在原因，但在危害分析和风险评估中对于功能异常表现的分析时，不需要考虑这些原因。

注2：仅考虑与相关项功能异常表现相关的危害；假设其他充分独立的系统（外部措施）均正确工作。

6.4.2.4 如果在本章中所识别出的危害超出了 GB/T 34590 的范围（本文件第 1 章），应按照组织的特定流程处理这些危害。

注：由于这些危害超出了GB/T 34590的范围，因此本文件未提供有关这些危害的ASIL等级的合规性指导，对此类危害的分类按照适用的安全流程进行。

6.4.2.5 应确定相关的危害事件。

6.4.2.6 应识别危害事件的后果。

注：如果相关项层面的功能异常表现导致该相关项丧失多个功能，则场景分析和危害识别要考虑其综合影响。

示例1：制动系统（ESC）的功能丧失可能导致驾驶辅助功能同步无效。

示例2：整车供电系统的失效能导致同时丧失一系列功能，包括：“发动机扭矩”、“助力转向”及“前向照明”。

6.4.2.7 应确保所选择的运行场景列表的详细程度不会导致 ASIL 等级的不适当降低。

注：对一个危害来说，一个非常详细的关于车辆状况、道路条件和环境条件的运行场景列表（本文件6.4.2.1），会使得用于危害事件分类的场景的颗粒度更为精细。这可以更容易地评估可控性和严重度。然而，大量的不同运行场景可能导致相应地降低各自的暴露等级，从而导致不恰当地降低ASIL等级。这可以通过合并类似的场景来避免。

6.4.3 危害事件分类

6.4.3.1 应对在 6.4.2 中识别出的所有的危害事件进行分类，不含超出 GB/T 34590 范围的危害事件。

注：如果难以对一个给定的危害进行严重度（S）、暴露概率（E）或可控性（C）的分级，需要采取保守分级的方法，即，一旦分级存在合理的怀疑，就采用较高的S、E或C等级。

6.4.3.2 对于每一个危害事件，应基于确定的理由来预估潜在伤害的严重度。应按照表 1 为严重度指定一个 S0、S1、S2 或 S3 的严重度等级。

注1：危害事件的风险评估关注的是潜在的处于风险中的每个人受到的伤害情况——包括引起危害事件的车辆的驾驶员或乘客，以及其他潜在的处于风险中的人员，如骑自行车的人员、行人或其他车辆上的人员。附录B中介绍的简明损伤定级（AIS）可用于界定伤害的严重度；此外，附录B中还包括不同类型的严重度和事故的参考示例。

注2：严重度的分级可基于对多个伤害的综合性的考量，相比只考虑单一伤害的评估结果而言，这样可能会导致一个较高的严重度等级。

注3：对被评估中的运行场景，严重度预估要考虑事件发生的合理顺序。

注4：严重度的评级基于涉险人员的代表性样本。

表1 严重度等级

等级	S0	S1	S2	S3
描述	无伤害	轻度和中度伤害	严重的和危及生命的伤害（有存活的可能）	危及生命的伤害（存活不确定），致命的伤害

6.4.3.3 有的运行场景会导致伤害（例如事故），在此运行场景下，其相关项后续的功能异常表现会增加或无法减小所产生的伤害，在这种情况下，严重度的分级可以仅限于初始运行场景（例如事故）和相关项功能异常表现所产生的严重度差异。

示例1：如果事故的发生不是由相关项的功能异常表现导致，则严重度的分级不用考虑事故所产生的伤害。

示例2：被考虑的相关项包含用于减少碰撞所致伤害的安全气囊功能。如果事故发生时安全气囊未能正常打开，那么由碰撞导致的伤害可以被确定。如果相同事故中安全气囊正常打开可以将伤害降低到一个较低的严重度等级，那么，在严重度评级时只需考虑两者的差异。

6.4.3.4 如果经过危害分析和风险评估，确定相关项的功能异常表现的后果明显仅限于物体损坏并不涉及对人员的伤害，则该危害的严重度等级可为 S0。如果一个危害事件的严重度等级为 S0，则无需分配 ASIL 等级。

6.4.3.5 对于每一个危害事件，应基于确定的理由预估每个运行场景的暴露概率。按照表 2，应为暴露概率指定一个 E0、E1、E2、E3 或 E4 的概率等级。

注1：从E1到E4等级，两个相邻E等级间的概率差异是一个数量级。

注2：暴露度的确定基于目标市场中有代表性的运行场景样本。

注3：暴露概率的更多信息和示例本文件附录B。

表2 关于运行场景的暴露概率等级

等级	E0	E1	E2	E3	E4
描述	不可能	非常低的概率	低概率	中等概率	高概率

6.4.3.6 当预估暴露概率时，不应考虑装备该相关项的车辆数量。

注：暴露概率的评估是基于假设每个车辆都配备有该相关项进行的。这意味着“因为该相关项未装备在每台车辆上（只有一些车辆装备该相关项），所以暴露概率会降低”的观点是不成立的。

6.4.3.7 暴露概率等级 E0 可用于在危害分析和风险评估过程中所建议的那些认为是难以置信的场景，无需进一步探讨。应记录排除这些场景的理由。如果一个危害事件的暴露度等级被指定为 E0，则无需分配 ASIL 等级。

示例：E0 可用于“不可抗力”风险的情况（本文件 B.3）。

6.4.3.8 对于每一个危害事件，应基于一个确定的理由预估驾驶员或其他处于运行场景的人员对该危害事件的可控性。应按照表 3 为可控性指定一个 C0、C1、C2 或 C3 的可控性等级。

注1：从C1至C3等级，两个相邻C等级间的概率差异是一个数量级。

注2：可控性评估是指对人员能够充分控制危害事件以避免特定伤害概率的预估。因此，使用级别分别为C0，C1，C2和C3的参数C，以对避免伤害的可能性进行分类。 假设驾驶员处于正常的状态（例如，驾驶员不疲劳），接受了恰当的驾驶员培训（驾驶员有驾驶执照）并且遵守所有适用的法律法规，包括应有的谨慎以避免为其他交通参与者带来风险。表B.6中列出了一些示例，这些示例对这些等级做出解释。

注3：要考虑合理可预见的误用，例如“作为一种常见的行为，没有与前方车辆保持所需的距离”。

注4：当危害事件与车辆方向和速度的控制无关时，例如肢体卡在运动部件中，该可控性是对涉险人员能够从危害场景中移出自身或被其他人员移出的概率预估。当考虑可控性时，要注意的是涉险人员可能不熟悉相关项的操作，或者可能没有意识到潜在的危害情况的发生。

注5：当可控性涉及多个交通参与者的行为时，可控性评估可以基于带有功能异常相关项的车辆的可控性，以及其他参与者的假定行为。

表3 可控性等级

等级	C0	C1	C2	C3
描述	可控	简单可控	一般可控	难以控制或不可控

6.4.3.9 如果相关项不可用的危害不影响车辆的安全运行（例如一些驾驶员辅助系统），或者可以通过常规的驾驶员行为来避免事故，则该危害事件的可控性等级可为 C0。如果一个危害事件的可控性等级为 C0，则无需分配 ASIL 等级。

示例1：如果试图开车出门时，在车库中发生了动力丢失的情况，可以选择 C0，因为任何驾驶员都可以把车停回车库。

注：在选择合适的可控性等级时，若有适用于相关危害事件的专用法规规定了其功能性能，并有证据（例如真实的使用体验）支撑，则该法规可以作为理由的一部分。

示例2：某个包含了车辆系统认证要求的专用法规，精确地定义了在失效情况下车辆系统应具备的力或加速度。

6.4.3.10 每一个危害事件的 ASIL 等级基于严重度、暴露概率和可控性的分级，并按照表 4 来确定。

注1：4个ASIL等级：ASIL A、ASIL B、ASIL C和ASIL D，其中ASIL A是最低的安全完整性等级，ASIL D是最高的。

注2：除了这4个ASIL等级之外，QM（质量管理）等级表示GB/T 34590不做要求。然而，相应的危害事件可能会影响安全，这种情况下需制定安全要求。QM等级表明质量流程足以管理已识别的风险。

表4 ASIL 等级确定

严重度等级	暴露度等级	可控性等级		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM

严重度等级	暴露度等级	可控性等级		
		C1	C2	C3
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A[a]
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D
本文件 6.4.3.11				

6.4.3.11 如果几种不太可能的场景组合导致暴露概率低于 E1，即使危害事件达到 S3 和 C3 仍然可以认定为 QM。

示例1：对于高压系统错误供电的功能异常，组合运行场景是：

——导致安全气囊点爆的碰撞；

——车辆的一部分处于水中；及

——高压系统部分暴露，没有造成内部短路。

示例2：对于燃油泵错误供应汽油的功能异常，组合运行场景是：

——导致安全气囊点爆的碰撞；

——泵后面的油箱系统保持功能齐全；

——泵的燃油管路破裂，以致汽油会滴在热部件上；及

——泵的能源供应功能齐全。

6.4.4 安全目标的确定

6.4.4.1 应为具有 ASIL 等级的每个危害事件确定一个安全目标，该 ASIL 等级从危害分析和风险评估中得出。如果所确定的安全目标是类似的，可将其合并为一个安全目标。

注：安全目标是相关项最高层面的安全要求。安全目标导出功能安全要求，以避免每个危害事件的不合理风险。安全目标不表述为技术解决方案，而表述为功能目的。

6.4.4.2 为危害事件所确定的 ASIL 等级应分配给对应的安全目标。如果将类似的安全目标合并为一个安全目标，按照 6.4.4.1，应将最高的 ASIL 等级分配给合并后的安全目标。

6.4.4.3 安全目标连同它们的 ASIL 等级应按照 GB/T 34590.8-XXXX 中第 6 章来定义。

注：安全目标可定义故障容错时间间隔，或物理特性（例如最大的非预期方向盘转矩，最大的非预期加速度），如果它们与ASIL等级的确定相关。

6.4.4.4 对于与确定 ASIL 等级（如果适用，包括定级为 QM 或没有分配 ASIL 等级的危害事件）相关的危害分析和风险评估过程，应识别其使用到的或从中得出的假设。对于所集成的相关项，应按照 GB/T 34590.4-XXXX 第 8 章对这些假设进行确认。

注：如有，在HARA中考虑的假设包括：驾驶员或处于风险中的人员的假定行为以及外部措施的相关假设。

6.4.5 T&B 车辆危害分析和风险评估的差异管理

6.4.5.1 6.4.5 中的要求仅适用于 T&B 车辆。

6.4.5.2 在对 T&B 车辆进行危害分析和风险评估时，必须考虑如下差异：

a) 基础车辆的类型；

b) T&B 车辆的配置；及

c) T&B 车辆的运行状态。

注：在选择差异类型用于分析时，采用工程判断是适当的。

示例1：车轮打滑可能仅与空载卡车相关，然而卡车空载的情况不像负载情况那样常见，因此会影响暴露概率。

示例2：与无挂车的情况比较，有挂车时驾驶员对某些危害的控制能力会降低，因此会影响可控性。

示例3：不同 T&B 车辆的车身安全性能有所不同，因此会影响严重度。

6.4.5.3 在进行危害分析和风险评估时，应考虑基础车辆的每一种相关类型。

6.4.5.4 在预估暴露概率时，不应考虑给定类型的基础车辆的数量。

6.4.5.5 在预估暴露概率时，不应考虑装备特定配置的车辆的数量。

6.4.5.6 在进行危害分析和风险评估时，应考虑对技术参数产生影响的运行场景的差异。

注1：车辆的用途是要考虑的运行场景的一部分，并在预估暴露概率时考虑。

示例1：驾驶没有半挂车的牵引车会导致驱动轴（技术参数）处于低负荷状态，这会降低车辆的动态稳定性。当预估暴露概率时，参考表 B.4，例如：“在公共道路上驾驶没有半挂车的牵引车”的运行场景，对其暴露概率等级评估为 E2。

注2：当进行危害分析与风险评估时，车身可以用于装载货物，需要考虑货物的变化情况。

示例2：负载条件（满载、部分负载、空载）以及重心位置的变化。

注3：车辆上装设备的功能，尤其是机械功能，可属于其他安全标准的范围。这些功能的危害分析与风险评估遵循特定适用的安全标准来进行。

注4：对设计用于支持特定车身应用的整车功能，危害分析和风险评估中可考虑车身的运行场景。

6.4.5.7 进行严重度、暴露度与可控性分级时，应考虑相关项的差异类型的适当组合。

注：适当的组合可基于工程判断来确定。

6.4.6 验证

6.4.6.1 应按照 GB/T 34590.8-XXXX 第 9 章对危害分析和风险评估包括安全目标进行验证，以提供证据证明：

a) 对运行场景和危害识别（及 T&B 车辆配置）选择的适用性；
b) 与相关项定义的符合性；
c) 与其他相关项相关的危害分析和风险评估的一致性；
d) 对危害事件覆盖的完备性；及
e) 分配了 ASIL 等级的安全目标与相关危害事件的一致性。

6.5 工作成果

6.5.1 危害分析和风险评估报告，由 6.4.1～6.4.5 的要求得出。

6.5.2 危害分析和风险评估验证报告，由 6.4.6 的要求得出。

7 功能安全概念

7.1 目的

本章的目的是：

a) 按照安全目标，定义相关项功能行为或降级的功能行为；
b) 按照安全目标，定义用于合理、及时地探测和控制相关故障的约束条件；
c) 定义相关项层面的策略或者措施，通过相关项自身、驾驶员或外部措施来实现要求的故障容错，或者充分减轻相关故障的影响；
d) 分配功能安全要求给系统架构设计或者外部措施；及
e) 根据接受准则，验证功能安全概念和定义安全确认准则。

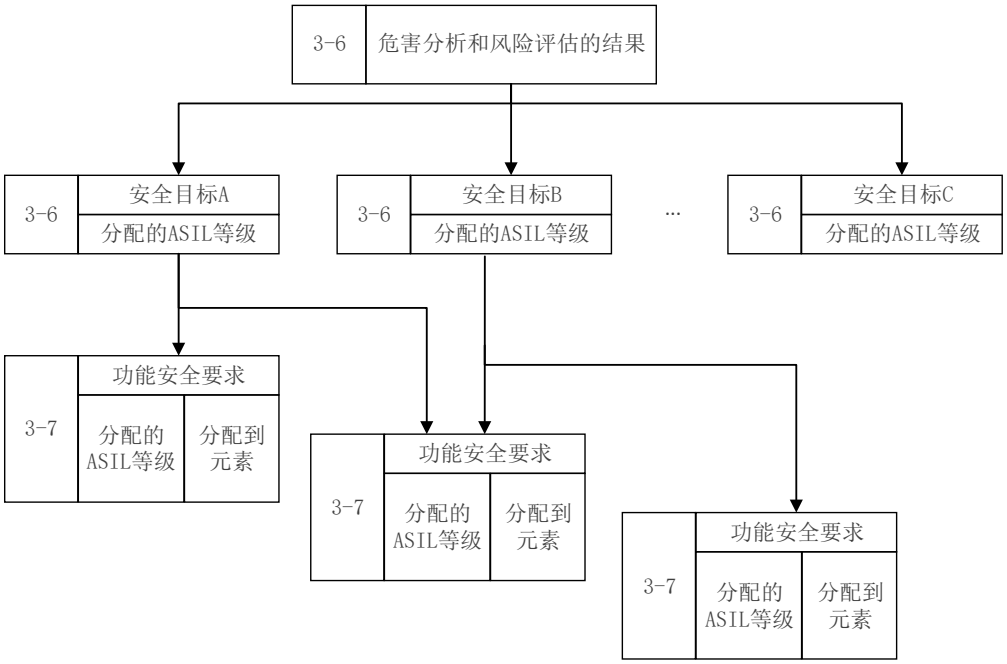
7.2 总则

为了满足安全目标，功能安全概念包括安全措施(含安全机制)，这些安全措施将在相关项的架构要素中实现，并在功能安全要求中规定。

图2说明了通过分层的方法，从危害分析和风险评估中得出安全目标，再由安全目标得出功能安全要求并将安全要求分配到系统架构设计。

使用初步架构设想为在早期开发阶段处理不成熟的架构信息提供了一种方法。

GB/T 34590相应部分安全要求的结构和分布本文件GB/T 34590.8-XXXX，图2。



注：图中GB/T 34590每部分的特定章节用以下方式标示：“m-n”，“m”代表部分号，“n”代表章号，例如“3-6”代表GB/T 34590.3的第6章。

图2 安全目标和功能安全要求层级

7.3 本章的输入

7.3.1 前提条件

应具备以下信息：

——相关项定义，按照 5.5.1。

——危害分析和风险评估报告，按照 6.5.1；及

——系统架构设计（来自外部）。

7.3.2 支持信息

可考虑以下信息：

无。

7.4 要求和建议

7.4.1 总则

功能安全要求应按照GB/T 34590.8-XXXX第6章进行定义。

7.4.2 功能安全要求的导出

7.4.2.1 功能安全要求应由安全目标导出，并考虑系统架构设计

7.4.2.2 应为每一个安全目标导出至少一项功能安全要求。

注：同一个功能安全要求可以由几个不同的安全目标导出（本文件图2）。

7.4.2.3 如果适用，功能安全要求应为以下内容定义策略：

a) 故障避免；

b) 故障探测、对故障或其导致的功能异常表现的控制；

c) 如果适用，从一个安全状态过渡到另一个安全状态；

d) 故障容错；

e) 故障情况下的功能降级，及其与 f）或 g）的交互。

示例：将车辆保持在跛行模式，直到点火开关从“开”切换到“关”。

f) 将风险暴露时间缩短到可接受时间所需的驾驶员警告；

g) 增加驾驶员可控性所需的驾驶员警告（例如发动机功能异常指示灯，ABS 故障报警灯）；

h) 如何满足整车层面的时间要求，即，如何定义故障处理时间间隔来满足故障容错时间间隔；及

i) 避免或减轻因不当仲裁了不同功能同时产生的多个控制请求而导致的危害事件。

注：列出项目c）、e）、f）和g）可以作为报警和降级策略的一部分。

7.4.2.4 如果适用，应考虑以下内容来定义每项功能安全要求：

a) 运行模式；

b) 故障容错时间间隔；

c) 安全状态；

d) 紧急运行时间间隔；及

e) 功能冗余（例如故障容错）。

注：为了制定一套完整有效的功能安全要求，安全分析（例如FMEA、FTA、HAZOP）可为以上活动提供支持。

7.4.2.5 如果可以通过过渡到或保持一个或多个安全状态来避免安全目标的违背，那么应定义相应的安全状态。

示例：一个安全状态可以是发生失效时在规定的时间内“关闭”、“锁定”、“车辆静止并保持”或“功能降低”。

7.4.2.6 如果在一个可接受的时间间隔内，不能过渡到安全状态，应定义紧急运行。

7.4.2.7 如果为了避免违反安全目标而对驾驶员或其他人员的必要行动做出了假设，则应：

注1：这些行动包括在可控性预测期间被认为是具有可信度的那些行动，以及在实施安全要求之后为满足安全目标所做的任何进一步的必要行动。

示例：自适应巡航控制：当驾驶员踩下加速踏板时，ACC 产生的制动被抑制。

a) 在功能安全概念中应定义这些行动；及

b) 在功能安全概念中应定义可供驾驶员或其他人员使用的足够的方法和控制手段

注2：对驾驶员的工作任务分析有助于考虑防止驾驶员超负荷，防止驾驶员的惊吓或恐慌（丧失控制车辆的能力）和模式混淆（关于操作模式的不正确的假设）。

注3：报警和降级策略的定义、驾驶员和其他潜在涉险人员的必要行动是用户手册的一种可能输入（本文件GB/T 34590.7-XXXX第5章）。

7.4.2.8 功能安全要求应分配给系统架构设计中的要素：

a) 在分配要求时，ASIL 等级和 7.4.2.4 中所给出的信息应从相关的安全目标中继承得到。如果应用了 ASIL 等级分解，则适用 GB/T 34590.9-XXXX 中第 5 章的要求；

b) 如果按照 GB/T 34590.9-XXXX 中第 6 章，无法证明系统架构设计中实施安全要求的各要素之间免于干扰，则这些架构要素应按照所实施安全要求中最高的 ASIL 等级进行开发；

c) 如果相关项包含多个电气/电子系统，则应根据系统架构设计定义各个电气/电子系统以及系统之间接口的功能安全要求。这些功能安全要求应分配到各个电气/电子系统中；

d) 如果相关项包含多个电气/电子系统，则可按照 GB/T 34590.4-XXXX，6.4.5.2 的要求，定义相应的随机硬件故障度量目标值 （本文件 GB/T 34590.5-XXXX 第 8 章和第 9 章）并分配给各个电气/电子系统。

注1：按照系统架构设计定义电气/电子系统的目标值，并在各开发阶段进行细化。

e) 如果在功能安全要求分配期间进行 ASIL 等级分解，则应按照 GB/T 34590.9-XXXX 中第 5 章的要求。

注2：独立性可通过对相关失效分析来验证（本文件GB/T 34590.9-XXXX第7章）。

7.4.2.9 如果功能安全概念依赖于其他技术的要素，则以下内容应适用：

a) 应导出基于其他技术的要素所实现的功能安全要求，并将其分配给架构中的相关要素；

b) 应定义与其他技术要素的接口相关的功能安全要求；

c) 应通过特定的措施（超出 GB/T 34590 的范围）来保证基于其他技术的要素所实现的功能安全要求；及

d) 无需对分配给这些要素的安全要求分配 ASIL 等级.

注1：对于分配给采用其他技术的要素的安全要求，可以定义合适的安全属性。可以参考GB/T34590.9第5章中描述的ASIL等级分解的概念，将功能安全要求分配给这些要素。这样，除了GB/T34590以外的采用其他技术的要素，也定义了恰当的实现和验证规则。

注2：各在安全确认活动期间需要提供证据证明，采用其他技术的要素是充分的。（本文件GB/T 34590.4第8章）

7.4.2.10 如果功能安全概念依赖于外部措施，则以下内容应适用：

a) 应导出并传达由外部措施实施的功能安全要求；

b) 应规定与外部措施接口的功能安全要求；及

c) 如果外部措施由一个或多个电气/电子系统实施，则应按照 GB/T 34590 指定功能安全要求。

注：在安全确认活动期间需要提供证据证明外部措施是充分的（本文件GB/T 34590.4-XXXX第8章）。

7.4.3 安全确认准则

7.4.3.1 应基于功能安全要求和安全目标对相关项安全确认的接受准则进行定义。

注1：关于详细准则和待确认特性列表的进一步要求（本文件GB/T 34590.4-XXXX第8章）。

注2：虽然安全目标的安全确认在V模型的右上角，但包含在开发过程的活动中，而不仅仅在开发结束时执行。

7.4.4 功能安全概念的验证

7.4.4.1 功能安全概念应按照 GB/T 34590.8-XXXX 中第 9 章进行验证，提供证据证明：

a) 其与安全目标的一致性和符合性；

b) 满足接受准则；及

c) 减轻或避免危害的能力。

注1：在概念阶段，可以对减轻或避免危害事件的能力进行验证，来评估安全概念并指出概念改进之处。此验证可与安全确认中使用的方法相同。然而，安全确认（以满足GB/T 34590.4-XXXX第8章要求）不能只基于概念研究（例如，原型）。

示例：减轻或避免危害的能力，可通过测试、试运行或专家判断来评估，可结合原型、研究报告、专项测试或仿真。

注2：针对该故障的特性（例如，是瞬态的或者是永久的），对减轻或避免危害的能力进行验证。

注3：对于验证，可使用一种基于可追溯性的论据，即，如果相关项符合功能安全要求，则该相关项符合安全目标。

7.5 工作成果

7.5.1　功能安全概念，由 7.4.1～7.4.3 的要求得出。

7.5.2　功能安全概念验证报告，由 7.4.4 的要求得出。

附 录 A
（资料性）
概念阶段的概览和工作流

表A.1提供了概念阶段的目的、前提条件和工作成果的概览。

表A.1 概念阶段概览

章	目的	前提条件	工作成果
5 相关项定义	本章的目的是： a）定义并描述相关项及其功能，对驾驶员、环境和其他相关项在整车层面上的依赖性和交互；及 b）为充分理解相关项提供支持，以便执行后续阶段的活动	无	5.5.1 相关项定义，由5.4要求得出
6 危害分析和风险评估	本章的目的是： a)识别并分类由相关项中的功能异常表现引起的危害事件; b）定义接受准则，包括危害行为的安全度量，以及由接受准则导出安全确认目标，用于评估残余风险;及 c)制定防止危害事件发生或减轻危害程度的安全目标及其相应的 ASIL 等级，以避免不合理的风险。	相关项定义（本文件5.5.1）	6.5.1 危害分析和风险评估报告，由6.4.1～6.4.5要求得出； 6.5.2 危害分析和风险评估的验证报告，由6.4.6要求得出
7 功能安全概念	本章的目的是： a）按照安全目标，定义相关项功能行为或降级的功能行为； b）按照安全目标，定义用于合理、及时地探测和控制相关故障的约束条件； c）定义相关项层面的策略或者措施，通过相关项自身、驾驶员或外部措施来实现要求的故障容错，或者充分减轻相关故障的影响； d）分配功能安全要求给系统架构设计或者外部措施；及 e）根据接受准则，验证功能安全概念和定义安全确认准则。	相关项定义（本文件5.5.1）； 危害分析和风险评估报告（本文件6.5.1）； 系统架构设计（来自外部）	7.5.1 功能安全概念，由7.4.1～7.4.3的要求得出； 7.5.2 功能安全概念验证报告，由7.4.4的要求得出。

附 录 B
（资料性）
危害分析和风险评估

B.1 总则

本附录给出了危害分析和风险评估的一般解释。B.2（严重度）、B.3（暴露概率）和B.4（可控性）中的例子仅供参考，并非穷尽。

对于这种分析方法，风险（R）可以被描述为一个包含三个参数的函数（F）：危害事件发生频率（f），可控性（C），即，所涉及人员通过及时反应以避免特定的伤害或损坏的能力，以及所产生的伤害或损坏的潜在严重度（S）：

$$R = F(f, C, S) \quad \text{(B.1)}$$

发生频率f依次受到两个因素的影响。要考虑的因素之一是人们以何种频度及多长时间能够发现他们自己处于上述危害事件可能发生的场景中。在GB/T 34590中，它被简化成会出现危害事件的运行场景发生概率的度量（暴露度，E）。另一个因素是相关项中故障的发生率，这在危害分析和风险评估中是不考虑的。然而，在危害分析与风险评估中由E, S, C的分级而得出的ASIL等级，确定了相关项最低限度的要求，以控制或减少随机硬件失效的概率，并且避免系统性故障。在风险评估中，不认为相关项的失效率是推理演绎的，因为可通过实现所得出的安全要求来避免不合理的残余风险。

危害分析与风险评估子阶段包括下述三个步骤。

a) 场景分析和危害识别（本文件 6.4.2）：场景分析和危害识别的目的是识别出可能会导致危害事件的相关项的潜在非预期行为。场景分析和危害识别活动需要一个关于相关项、相关项功能和边界的清晰定义。场景分析和危害识别是基于相关项的行为，因此并不一定需要知道相关项的设计细节。

示例：场景分析和危害识别考虑的要素可包括：

——车辆的使用场景，如高速行驶、城市行驶、停车、越野；

——环境条件，如路面摩擦、侧风；

——合理可预见的驾驶员使用和误用；

——运行系统之间的交互；及

——T&B 的基础车辆、车辆配置和车辆运行。

b) 危害事件的分类（本文件 6.4.3）：危害分类方案包括与相关项危害事件相关的严重度、暴露概率以及可控性的确定。严重度代表对一个特定驾驶场景中的潜在伤害的预估，而暴露概率是由相应的场景来确定的。可控性衡量了驾驶员或其他道路交通参与者在所考虑到的运行场景中避免所考虑到的事故的难易程度。对于每一个危害，基于相关危害事件的数量，该分类将导出严重度、暴露概率和可控性的一个或多个组合。

c) ASIL 等级确定（本文件 6.4.3）：确定所需的汽车安全完整性等级。

B.2 严重度示例

B.2.1 总则

评估危害对驾驶员、乘客、车辆周围人员或周边车辆中人员产生的潜在伤害，以确定相应危害的严重度等级，如表B.1所示。

表B.1给出了示例，关于一个给定危害可能导致的后果，以及每一个后果的严重度等级。

由于事故的复杂性以及事故场景的多样性，表B.1中所提供的例子仅代表对事故后果的一个大概估计。它们代表根据过往事故分析所得到的预期值，因此，不能通过这些单独的描述来得出一个普遍有效的结论。

事故统计可用于确定不同类型事故中预期发生的伤害的分布。

在表B.1中，AIS表示伤害等级分类，但仅用于单一伤害。除AIS外，也可以使用其他分类方法，例如最大简明损伤定级 （MAIS，Maximum AIS）和创伤严重度评分（ISS，Injury Severity Score）。

特定伤害等级的使用依赖于同期所进行的医学研究的进展情况。因此，不同伤害等级，例如AIS、ISS和NISS的适用性可以随时间而变化（本文件参考文献[3],[5],[6]）。

B.2.2 AIS等级描述

使用AIS分级来描述严重度。AIS代表受伤的严重程度分级，它由汽车事故医学高级协会（AAAM，Association for the Advancement of Automotive Medicine）发布。该指南的创建使得国际间的严重度比较成为可能。AIS等级分为七级：

——AIS 0：无伤害；

——AIS 1：轻伤，例如皮肤表面伤口、肌肉疼痛、挥鞭样损伤等；

——AIS2：中度伤害，例如深度皮肉伤、脑震荡长达 15 分钟无意识、单纯性长骨骨折、单纯性肋骨骨折等；

——AIS 3：严重，但未危及生命的伤害，例如无脑损伤的颅骨骨折、没有脊髓损伤的第四颈椎以下脊柱错位、没有呼吸异常的超过一根的肋骨骨折等；

——AIS 4：严重伤害（危及生命、有生存的可能），例如伴随或不伴随颅骨骨折的脑震荡引起的长达 12 小时的昏迷、呼吸异常；

——AIS 5：危险伤害（危及生命，生存不确定），例如伴随脊髓损伤的第四颈椎以下脊柱骨折、肠道撕裂、心脏撕裂、伴随颅内出血的超过 12 小时的昏迷等；

——AIS 6：极度危险或致命伤害，例如伴随脊髓损伤的第三颈椎以上脊柱骨折、极度危险的体腔（胸腔和腹腔）开放性伤口等。

表B.1 严重度等级举例

严重程度等级（见表1）	S0	S1	S2	S3
描述	无伤害	轻度和中度伤害	严重的和危及生命的伤害（有存活的可能）	危及生命的伤害（存活不确定），致命的伤害
对单一伤害的参考(根据AIS分级)	AIS 0及AIS 1-6可能性小于10%；或不能被归为安全相关的损害	AIS 1-6可能性大于10%（不属于S2和S3）	AIS 3-6可能性大于10%（不属于S3）	AIS 5-6可能性大于10%
示例	——冲撞路边设施； ——撞倒路边邮筒、 围栏等； ——轻微刮痕损害； ——在进入或退出停车位置时损害； ——没有碰撞或者侧翻的情景下离开道路	——侧面碰撞一个狭窄的静止物体，例如乘用车以非常低的速度撞上一棵树（影响到乘员舱）； ——以非常低的速度和其他乘用车后碰/正碰；	——侧面碰撞一个狭窄的静止物体，例如乘用车以低速撞上一棵树（影响到乘员舱）； ——以低速和其他乘用车后碰/正碰；	——侧面碰撞一个狭窄的静止物体，例如乘用车以中速撞上一棵树（影响到乘员舱）； ——以中速和其他车辆后碰/正碰；

严重程度等级（见表1）	S0	S1	S2	S3
		——没有乘员舱变形的正面碰撞（例如追尾其他车辆、半挂车）	——以低速造成的行人或自行车事故	——有乘员舱变形的正面碰撞（例如追尾其他车辆、半挂车）
注：表B.1中的信息示例可应用于乘用车和T&B，但是要根据具体情况进行考虑。				

B.3 暴露概率的示例与解释

对暴露概率的预估需要场景评估，在这些场景中，会出现促成危害发生的相关环境因素。需要评估的场景包括各种驾驶或运行场景。

评估的结果会确定危害场景的暴露概率级别，暴露概率级别有5个，分别为E0（最低暴露度级别）、E1、E2、E3、E4（最高暴露度级别）。

那些尽管在危害分析和风险评估中被定义了，但又被认为是不寻常或令人难以置信的场景会被指定为E0。仅仅与E0场景关联的危害的后续评估会被排除在进一步的分析之外。

示例1：典型的 E0 示例：

a） 极其不寻常的或不可能同时发生的情况，例如车辆涉及到在高速公路上降落的飞机的事故；及

b） 自然灾害，如地震、飓风、森林大火。

根据场景的持续时间（重叠时间）或发生的频率，将其余的E1、E2、E3和E4等级指定给可发生危害的场景。

注1：可依据例如地理位置或使用类型等来分级（本文件 6.4.3.5）。

危害的暴露度（E）可通过两种方式进行预估。第一种是基于场景的持续时间，第二种是基于场景发生的频率。例如，一个危害可以与一个给定运行场景的持续时间相关，如用在通过交通路口的平均时间；而另一个危害可以与同一个运行场景的发生频率相关，如车辆重复通过交通十字路口的频率。

在第一种情况下，暴露度按照场景的持续时间分级，暴露概率通常根据所考虑的场景下花费的时间与总的运行时间（如上电）的比值来估算。注意，在某些情况下，总运行时间可以是汽车生命周期（包括下电）。在第二种情况下，一些暴露度的预估通过使用相关驾驶场景的发生频率来确定可能更为合适。一个合适的例子是，在这些情况下，场景发生后的很短的时间间隔内，已存在的电气/电子系统故障会导致危害事件的发生。

表B.2和B.4给出了按持续时间分级的驾驶场景和典型的暴露度分级的示例，表B.3和表B.5给出了按频率分级的驾驶场景示例。

除了这些驾驶场景外，还要考虑该运行场景的具体情况。根据导致危害事件的确切时间和确切位置确定实际的暴露度是必要的。

示例2：儿童锁自身的失效不一定会导致危害事件，除非儿童年龄足够大能够解开安全带并离开车辆进入交通流，而此时另一辆车正在靠近。

驾驶场景可能同时具有持续特性和频率特性，如在停车场驾驶。在这种情况下，在表B.2/B.4和B.3/B.5的例子可能无法得出相同的暴露度等级，所以最合适的暴露度等级是根据对所考虑的运行场景的分析而选取的。

如果失效维持在潜伏状态的时间长度与危害事件预期发生之前的时间长度是相当的，那么暴露概率的预估应考虑这个时间长度。典型的这会涉及到按需动作的设备，比如安全气囊。

在这种情况下，暴露概率可通过$\sigma \times T$来预估：σ是运行场景的发生率，T是失效未被感知的持续时间（可能长达车辆的整个生命周期）。当乘积结果较小时，近似值$\sigma \times T$是有效的。

注2：关于所考虑的失效的持续时间，危害分析和风险评估不考虑作为相关项一部分的安全机制（本文件6.4.1.2）。

表B.2 基于运行场景持续时间的暴露概率等级

运行场景暴露概率等级（见表2）	E1	E2	E3	E4
描述	极低概率	低概率	中等概率	高概率
持续时间（平均运行时间的百分比）	无定义	＜1%的平均运行时间	1%～10%的平均运行时间	＞10%的平均运行时间
道路类型示例	-	——乡间道路交叉口； ——高速公路出口匝道。	——单行道（城市道路）	——高速公路； ——乡间道路； ——城市道路。
路面类型示例	-	——冰雪路面； ——有很多光滑树叶的路面。	——湿滑路面	-
车辆静止状态类型示例	——车辆在跳线跨接启动期间； ——在维修厂。	——连接挂车； ——装备车顶行李架； ——车辆在加油。	——车辆在斜坡上（停在斜坡上）	-
驾驶操控类型示例	——下坡时关闭发动机（山路）	——倒车； ——超车； ——停车(有挂车连接)。	——交通拥挤（频繁起停）	——加速； ——减速； ——停在红绿灯前（城市道路）； ——变道（高速公路)。

表B.3 基于运行场景频率的暴露概率等级

运行场景暴露概率分级（见表2）	E1	E2	E3	E4
类型	极低概率	低概率	中等概率	高概率
场景发生的频率	对大多数驾驶员而言，一年发生的频率小于一次	对大多数驾驶员而言，每年发生几次	对普通驾驶员而言，基本上每个月发生一次或多次	平均几乎发生在每次驾驶中
道路类型示例	-	——山路，带有不安全的陡峭斜坡	-	-
路面类型示例	-	——冰雪路面	——湿滑路面	-
车辆静止状态类型示例	——停车,需要重新启动发动机(在铁路道口)； ——车辆被拖的过程中。	——装备车顶行李架	——车辆在加油； ——车辆在斜坡上（停在斜坡上）。	-
驾驶操控类型示例	-	——避让动作，偏离预期路线	——超车	——换挡； ——转弯（转向）； ——使用指示器； ——倒车行驶。

表B.4和B.5提供了T&B的示例。表中考虑了不同类型的基础车辆：

——长途运输车（LH），用于长途运输货物；

——配送车（DI），用于配送货物；
——专用作业车（VO），用于执行特定工作功能，如翻斗车、混凝土搅拌运输车、垃圾车；
——城市公交车(CB)，供城市和郊区使用;
——城市间巴士（IB），用于城市间交通；及
——长途汽车（CO），用于长途旅行。

表B.4 用于 T&B 的基于运行场景持续时间的暴露概率等级

运行场景暴露概率等级（见表2）		E1	E2	E3	E4
类型		极低概率	低概率	中等概率	高概率
持续时间（平均运行时间的百分比）		无定义	＜1%的平均运行时间	1%～10%的平均运行时间	＞10%的平均运行时间
示例	倒车行驶	-	长途运输车、城市公交车、长途汽车、城市间巴士	配送车、专用作业车	-
	以小的速度差超过另一辆卡车或公共汽车（变道至对向车道）	长途运输车、配送车、专用作业车、长途汽车、城市间巴士	-	-	-
	挂拖车行驶	-	-	配送车、长途汽车，城市间巴士	长途运输车、专用作业车
	没有牵引拖车的半挂车（在公共道路上）	-	-	长途运输车、配送车、专用作业车	-
	在施工现场驾驶（直接在施工现场驾驶车辆，而不是仅用于将货物运送至施工现场）	长途运输车	配送车	-	专用作业车
	陡坡	长途运输车、城市公交车	配送车、长途汽车、城市间巴士	专用作业车	-
	停在公共汽车站	-	-	长途汽车	城市公交车、城市间巴士
	驶入/驶出公共汽车站	-	长途汽车	城市公交车、城市间巴士	-
注：表B.2中的示例可用于T&B，但是要根据具体情况进行考虑。对于表B.2和表B.4中出现的情况，表B.4更适合T&B。					

表B.5 T&B 的基于运行场景频率的暴露概率等级

运行场景暴露概率等级（见表2）	E1	E2	E3	E4
描述	极低概率	低概率	中等概率	高概率
场景发生的频率	对大多数驾驶员而言，一年发生的频率小于一次	对大多数驾驶员而言，每年发生几次	对普通驾驶员而言，基本上每个月发生一次或多次	平均几乎发生在每次驾驶中

运行场景暴露概率等级（见表2）		E1	E2	E3	E4
示例	倒车行驶	-	-	城市公交车	长途运输车，配送车，专用作业车，长途汽车，城市间巴士
	以小的速度差超过另一辆卡车或公共汽车（变道至对向车道）	-	-	长途运输车，配送车，专用作业车，长途汽车，城市间巴士	-
	挂拖车行驶	-	-	配送车，长途汽车，城市间巴士	长途运输车，专用作业车
	没有牵引拖车的半挂车（在公共道路上）	-	配送车，专用作业车	长途运输车	-
	在施工现场驾驶（直接在施工现场驾驶车辆，而不是仅用于将货物运送至施工现场）	长途运输车	配送车	-	专用作业车
	陡坡	长途运输车，城市公交车	配送车，长途汽车，城市间巴士	-	专用作业车
	停在/驶入/驶出公共汽车站	-	-	-	城市公交车，长途汽车，城市间巴士
注：表B.3中的示例可用于T&B，但是要根据具体情况进行考虑。对于表B.3和表B.5中均出现的场景，表B.5更适合T&B。					

B.4 可控性示例

为确定一个给定危害的可控性等级，需要预估具有代表性的驾驶员或其他涉及人员为避免伤害发生而能对场景施加影响的可能性。

这种可能性预估包括：如果这个给定的危害将要发生，具有代表性的驾驶员能够保持或者重新控制车辆的可能性，或者在这个危害发生范围内的个体能够通过他们的行动来避免危害的可能性。这种考量基于这样的假设，即危害场景中的个体为保持或者重新控制当前情况采取的必要控制行为，以及所涉及的驾驶员采取有代表性的驾驶行为。

注1：可控性预估可能受到很多因素的影响，包括该目标市场的驾驶员概况，个体年龄、手眼配合、驾驶经验、文化背景等。

注2：可使用实验或分析过程进行预估。

为了有助于这些评估，表B.6提供了一些发生功能异常的驾驶场景示例，以及可能避免伤害的相应的控制行为的假设。这些场景对应到可控性的分级，明确了用于判断控制能力水平90%和99%的分隔点。

表B.6 驾驶员或者潜在涉险人员可能控制的危害事件示例

可控性等级(见表3)	C0	C1	C2	C3
描述	可控	简单可控	一般可控	难以控制或不可控

可控性等级(见表3)	C0	C1	C2	C3
驾驶因素和场景	常规可控	超过99%的普通驾驶员或交通参与者能够避免伤害	90%到99%普通驾驶员或交通参与者能够避免伤害	不到90%普通驾驶员或交通参与者能够避免伤害
分散注意力的情况示例，如：无线电音量意外增加或燃油不足报警信息	保持既定行驶路线	-	-	-
不影响车辆安全操作的驾驶员辅助系统失效示例	保持既定行驶路线	-	-	-
开车时非预期关闭车窗的示例	-	从车窗处移开手臂	-	-
从静止状态加速时转向柱锁止的示例	-	制动减速/停止车辆	-	-
紧急制动情况下ABS失效的示例	-	-	保持预期的行驶路线	-
高侧向加速度时驱动失效的示例	-	-	保持预期的行驶路线	-
乘客站在门口时无意中打开公交车门的示例	-	-	乘客抓住扶手以免掉下车	-
制动失效的示例	-	-	-	躲避行驶路径上的物体
高速行驶中驾驶员安全气囊误触发的示例	-	-	-	保持预期的行驶路线，留在车道里面；或制动减速/停车
制动时可能导致拖车过度摆动成V字型的示例	-	-	-	驾驶员反转向和刹车，以保持预期的行驶路线
处于高等级自动驾驶功能时驾驶员不在环的示例	-	-	-	未尝试保持预期的行驶路线

注1：对于C2，一个符合RESPONSE 3(本文件参考文献[4])的合理的测试场景是足够的：“实际的测试经验表明，每个场景20个有效的数据包能提供基本的有效性说明”。如果这20个数据包中的每一个都符合测试的通过标准，能够证明85%的可控性水平（达到一个通常能被人为因素测试接受的95%的置信度）。这为C2预估的合理性提供了适当的证据。

注2：对于C1，通过一个测试去提供一个99%的驾驶员都能够在特定的驾驶环境下“通过”这个测试的理由是不可行的，因为必须要有大量的测试项目作为这个理由的适当的证据。可以基于专家判断来决定。

注3：由于C3等级假定为没有可控性，所以对于这个分类理由不需要提供相关的适当证据。

注4：表B.6中的示例可应用于乘用车和T＆B车辆，但是要根据具体情况进行考虑。

参 考 文 献

[1] ISO 26262-12:2018, Road Vehicles — Functional Safety — Part 12: Adaptation of ISO 26262 for motorcycles.

[2] GB/T 20438-2017（所有部分）电气/电子/可编程电子安全相关系统的功能安全.

[3] Abbreviated injury scale; Association of the advancement of Automotive medicine; Barrington, IL, USA Information is also available at www.aaam.org.

[4] Code of Practice for the design and evaluation of ADAS, EU Project RESPONSE 3: Oct. 2006;https://www.acea.be/publications/article/code-of-practice-for-the-design-and-evaluation-of-adas.

[5] BAKER, S.P., O'NEILL, B., HADDON, W., LONG, W.B., The injury severity score: a method for describing patients with multiple injuries and evaluating emergency care, The Journal of Trauma, Vol. 14, No. 3, 1974.

[6] BALOGH, Z., OFFNER, P.J., MOORE, E.E., BIFFL, W.L., NISS predicts post injury multiple organ failure better than ISS, The Journal of Trauma, Vol. 48, No. 4, 2000.